REAL ALGEBRAIC GEOMETRY FOR MATRICES OVER COMMUTATIVE RINGS

J. CIMPRIČ

Abstract. We define and study preorderings and orderings on rings of the form $M_n(R)$ where R is a commutative unital ring. We extend the Artin-Lang theorem and Krivine-Stengle Stellensätze (both abstract and geometric) from R to $M_n(R)$. This problem has been open since the seventies when Hilbert's 17th problem was extended from usual to matrix polynomials. While the orderings of $M_n(R)$ are in one-to-one correspondence with the orderings of R, this is not true for preorderings. Therefore, our theory is not Morita equivalent to the classical real algebraic geometry.

1. Introduction

Real algebraic geometry studies sets of the form

$$K_{\{g_1,\ldots,g_m\}} = \{x \in \mathbb{R}^d \mid g_1(x) \geq 0, \ldots, g_m(x) \geq 0\},$$

where $d \in \mathbb{N}$ and $g_1, \ldots, g_m \in \mathbb{R}[x_1, \ldots, x_d]$, and the corresponding preorderings

$$T_{\{g_1,\ldots,g_m\}} = \{ \sum_{\varepsilon \in \{0,1\}^m} c_\varepsilon g_1^{\varepsilon_1} \cdots g_m^{\varepsilon_m} \mid c_\varepsilon \in \sum \mathbb{R}[x_1, \ldots, x_d]^2 \}.$$

Its most fundamental result is due to Krivine [4] and Stengle [10]:

Theorem A. *For every $f, g_1, \ldots, g_m \in \mathbb{R}[x_1, \ldots, x_d]$ we have that:*

(1) $K_{\{g_1,\ldots,g_m\}} = \emptyset$ *iff* $-1 \in T_{\{g_1,\ldots,g_m\}}$.
(2) $f(x) > 0$ *for every* $x \in K_{\{g_1,\ldots,g_m\}}$ *iff there exist* $t, t' \in T_{\{g_1,\ldots,g_m\}}$ *such that* $ft = 1 + t'$.
(3) $f(x) \geq 0$ *for every* $x \in K_{\{g_1,\ldots,g_m\}}$ *iff there exist* $t, t' \in T_{\{g_1,\ldots,g_m\}}$ *and* $k \in \mathbb{N}$ *such that* $ft = f^{2k} + t'$.
(4) $f(x) = 0$ *for every* $x \in K_{\{g_1,\ldots,g_m\}}$ *iff there exists* $k \in \mathbb{N}$ *such that* $-f^{2k} \in T_{\{g_1,\ldots,g_m\}}$.

Date: May 1, 2012.
1991 *Mathematics Subject Classification.* 14P, 13J30, 47A56.
Key words and phrases. positive polynomials, matrix polynomials, Positivstellensatz, real algebraic geometry.

Assertion (2) is called the Positivstellensatz, assertion (3) the Nichtnegativstellensatz and assertion (4) the semialgebraic Nullstellensatz.

The proof consists of two steps. Firstly, one defines the real spectrum of a commutative unital ring and proves an abstract version of the Krivine-Stengle theorem. Secondly, one proves that the real spectrum of $\mathbb{R}[x_1, \ldots, x_d]$ contains $\mathbb{R}^d$ as a dense subset (Artin-Lang Theorem).

Motivated by [8] and [9], we would like to extend this theory to matrix polynomials of fixed size $n \in \mathbb{N}$, i.e. from the ring $\mathbb{R}[x_1, \ldots, x_d]$ to the ring $\mathcal{M}_n(\mathbb{R}[x_1, \ldots, x_d])$ of all $n \times n$ matrices with entries from $\mathbb{R}[x_1, \ldots, x_d]$. We will consider sets of the form

$$K_{\{\mathbf{G}_1,\ldots,\mathbf{G}_m\}} = \{x \in \mathbb{R}^d \mid \mathbf{G}_1(x) \succeq 0, \ldots, \mathbf{G}_m(x) \succeq 0\}$$

where $\mathbf{G}_1, \ldots, \mathbf{G}_m$ belong to the set $\mathcal{S}_n(\mathbb{R}[x_1, \ldots, x_d])$ of all symmetric matrices from $\mathcal{M}_n(\mathbb{R}[x_1, \ldots, x_d])$ and "$\succeq 0$" means "is positive semidefinite". In Section 2 we will define the corresponding preordering $T_{\{\mathbf{G}_1,\ldots,\mathbf{G}_m\}} \subseteq \mathcal{S}_n(\mathbb{R}[x_1, \ldots, x_d])$ as the smallest quadratic module in $\mathcal{M}_n(\mathbb{R}[x_1, \ldots, x_d])$ which contains $\mathbf{G}_1, \ldots, \mathbf{G}_m$ and whose intersection with the set $\mathbb{R}[x_1, \ldots, x_d] \cdot \mathbf{I}_n$, where $\mathbf{I}_n$ is the identity matrix, is closed under multiplication. In Section 6 we will prove the following generalization of Theorem A.

Theorem B. *For every $\mathbf{F}, \mathbf{G}_1, \ldots, \mathbf{G}_m \in \mathcal{S}_n(\mathbb{R}[x_1, \ldots, x_d])$ we have that:*

1. $K_{\{\mathbf{G}_1,\ldots,\mathbf{G}_m\}} = \emptyset$ *iff* $-\mathbf{I}_n \in T_{\{\mathbf{G}_1,\ldots,\mathbf{G}_m\}}$.
2. $\mathbf{F}(x)$ *is positive definite for every* $x \in K_{\{\mathbf{G}_1,\ldots,\mathbf{G}_m\}}$ *iff there exist* $\mathbf{B}, \mathbf{B}' \in T_{\{\mathbf{G}_1,\ldots,\mathbf{G}_m\}}$ *such that* $\mathbf{F}\mathbf{B} = \mathbf{B}\mathbf{F} = \mathbf{I}_n + \mathbf{B}'$.
3. $\mathbf{F}(x) \succeq 0$ *for every* $x \in K_{\{\mathbf{G}_1,\ldots,\mathbf{G}_m\}}$ *iff there exist* $\mathbf{B}, \mathbf{B}' \in T_{\{\mathbf{G}_1,\ldots,\mathbf{G}_m\}}$ *and* $k \in \mathbb{N}$ *such that* $\mathbf{F}\mathbf{B} = \mathbf{B}\mathbf{F} = \mathbf{F}^{2k} + \mathbf{B}'$.
4. $\mathbf{F}(x) = 0$ *for every* $x \in K_{\{\mathbf{G}_1,\ldots,\mathbf{G}_m\}}$ *iff there exists* $k \in \mathbb{N}$ *such that* $-\mathbf{F}^{2k} \in T_{\{\mathbf{G}_1,\ldots,\mathbf{G}_m\}}$.

The element $\mathbf{B}$ from assertion (2) can always be chosen from the set $\mathbb{R}[x_1, \ldots, x_d] \cdot \mathbf{I}_n$ while the element $\mathbf{B}$ from assertion (3) cannot.

In Section 6 we will also prove an abstract version of Theorem B for rings of the form $\mathcal{M}_n(R)$ where R is a commutative unital ring and n is a positive integer. The points and the topologies of the real spectrum of the ring $\mathcal{M}_n(R)$ are defined in Sections 5 and 4 respectively. We will prove that the real spectrum of $\mathcal{M}_n(R)$ is homeomorphic to the real spectrum of R. This result will imply a variant of the Artin-Lang Theorem for the ring $\mathcal{M}_n(\mathbb{R}[x_1, \ldots, x_d])$.

The main step in the proof of Theorem B is the construction of polynomials $h_1, \ldots, h_r \in \mathbb{R}[x_1, \ldots, x_d]$ such that $K_{\{h_1\mathbf{I}_n,\ldots,h_r\mathbf{I}_n\}} = K_{\{\mathbf{G}_1,\ldots,\mathbf{G}_m\}}$ and $T_{\{h_1\mathbf{I}_n,\ldots,h_r\mathbf{I}_n\}} \subseteq T_{\{\mathbf{G}_1,\ldots,\mathbf{G}_m\}}$; see Proposition 5. From Theorem A

(applied to $\det(\mathbf{F}-\lambda\mathbf{I}_n)-(-\lambda)^n$ and $h_1,\ldots,h_r,-\lambda\in\mathbb{R}[x_1,\ldots,x_d,\lambda]$) and the Cayley-Hamilton Theorem we then deduce a slightly stronger version of the theorem with $T_{\{\mathbf{G}_1,\ldots,\mathbf{G}_m\}}$ replaced by $T_{\{h_1\mathbf{I}_n,\ldots,h_r\mathbf{I}_n\}}$. The advantage of the preordering $T_{\{h_1\mathbf{I}_n,\ldots,h_r\mathbf{I}_n\}}$ is that it is always finitely generated as a quadratic module while the advantages of the preordering $T_{\{\mathbf{G}_1,\ldots,\mathbf{G}_m\}}$ are that it always contains $\mathbf{G}_1,\ldots,\mathbf{G}_m$ and that it is uniquely determined by $\mathbf{G}_1,\ldots,\mathbf{G}_m$. Preorderings of the form $T_{\{h_1\mathbf{I}_n,\ldots,h_r\mathbf{I}_n\}}$ were already considered in [9, Chapter 4] but their version of the matrix Krivine-Stengle Theorem is not related to ours.

The last claim of Theorem B (about denominators in $\mathbb{R}[x_1,\ldots,x_d]\cdot\mathbf{I}_n$) does not follow from other claims. The first part is proved by induction on n using Schur complements; see [1]. For the second part see Example 4. It would be interesting to know if the element $\mathbf{B}$ from assertion (3) can be chosen from the set $\mathbb{R}[x_1,\ldots,x_d]\cdot\mathbf{I}_n$ if $m=0$ (i.e. in the case of no constraints)[1]. Then Theorem B would imply Artin's Theorem for matrix polynomials (see [3] or [6] or [9, Proposition 10]).

2. Quadratic modules and preorderings

Let n be a positive integer, R a commutative unital ring and $\mathcal{M}_n(R)$ the ring of all $n\times n$ matrices over R with transposition as the involution. The unit of $\mathcal{M}_n(R)$ is the identity matrix $\mathbf{I}_n$ and the center $\mathcal{Z}_n(R)$ of $\mathcal{M}_n(R)$ is equal to $R\cdot\mathbf{I}_n$. We also assume that R has the trivial involution, hence it can be identified as a $*$-ring with both $\mathcal{Z}_n(R)$ and $\mathcal{M}_1(R)$. We will use the following notation: lower case letters for elements of R, upper case letters for subsets of R, bold lower case letters for vectors over R, bold upper case letters for matrices over R, calligraphic letters for sets of matrices and fracture letters for families of sets of matrices.

Let $\mathcal{S}_n(R):=\{\mathbf{A}\in\mathcal{M}_n(R)\mid\mathbf{A}^T=\mathbf{A}\}$ be the set of all symmetric $n\times n$ matrices over R. A subset $\mathcal{M}$ of $\mathcal{S}_n(R)$ is a *quadratic module* if $\mathbf{I}_n\in\mathcal{M}$, $\mathcal{M}+\mathcal{M}\subseteq\mathcal{M}$ and $\mathbf{A}^T\mathcal{M}\mathbf{A}\subseteq\mathcal{M}$ for every $\mathbf{A}\in\mathcal{M}_n(R)$. The smallest quadratic module which contains a given subset $\mathcal{G}$ of $\mathcal{S}_n(R)$ will be denoted by $\mathcal{M}^n_{\mathcal{G}}$. It consists of all finite sums of elements of the form $\mathbf{A}^T\mathbf{G}\mathbf{A}$ where $\mathbf{G}\in\mathcal{G}\cup\{\mathbf{I}_n\}$ and $\mathbf{A}\in\mathcal{M}_n(R)$. In particular, a subset M of R is a quadratic module if $1\in M$, $M+M\subseteq M$ and

[1]Note added in press. Aljaž Zalar recently showed that the answer to this question is negative. I would like to thank him for allowing me to include his example here. For $\mathbf{F}$ he takes a diagonal 2×2 matrix with entries p and 1 where p is a psd form such that every form h for which h^2p is sos must have a zero (see [7], the last paragraph in Section 2). Then he proceeds as in Example 4.

$r^2 M \subseteq M$ for every $r \in R$. The smallest quadratic module in R which contains a given subset G of R will be denoted by M_G.

Let $\mathbf{E}_{ij}$ be the coordinate matrices in $\mathcal{M}_n(R)$, let $\mathbf{e}_i$ be the coordinate vectors in R^n and let $p\colon \mathcal{M}_n(R) \to R$ be the mapping defined by

$$p(\mathbf{A}) = \mathbf{e}_1^T \mathbf{A} \mathbf{e}_1.$$

Lemma 1.

(1) *For every quadratic module $\mathcal{M}$ in $\mathcal{M}_n(R)$, we have that $\mathcal{M} \cap \mathcal{Z}_n(R) = p(\mathcal{M}) \cdot \mathbf{I}_n$.*
(2) *For every subset $\mathcal{G}$ of $\mathcal{S}_n(R)$, we have that $p(\mathcal{M}^n_{\mathcal{G}}) = M_{\mathcal{G}'}$ where $\mathcal{G}' = \{\mathbf{v}^T \mathbf{G} \mathbf{v} \mid \mathbf{G} \in \mathcal{G}, \mathbf{v} \in R^n\}$, and so $\mathcal{M}^n_{\mathcal{G}} \cap \mathcal{Z}_n(R) = M_{\mathcal{G}'} \cdot \mathbf{I}_n$.*

Proof. (1) If $\mathbf{A} \in \mathcal{M} \cap \mathcal{Z}_n(R)$, then $\mathbf{A}$ is a scalar matrix, hence $\mathbf{A} = p(\mathbf{A})\mathbf{I}_n$, so $\mathbf{A} \in p(\mathcal{M})\mathbf{I}_n$. Conversely, if $\mathbf{A} \in p(\mathcal{M})\mathbf{I}_n$, then $\mathbf{A}$ is a scalar matrix, hence it belongs to $\mathcal{Z}_n(R)$. Moreover, for some $\mathbf{M} \in \mathcal{M}$, $\mathbf{A} = p(\mathbf{M})\mathbf{I}_n = \sum_{i=1}^n \mathbf{E}_{1i}^T \mathbf{M} \mathbf{E}_{1i} \in \mathcal{M}$.

(2) We have that $p(\mathcal{M}^n_{\mathcal{G}}) = \{p(\mathbf{M}) \mid \mathbf{M} \in \mathcal{M}_{\mathcal{G}}\} = \{p(\sum_{i,j} \mathbf{A}_{ij}^T \mathbf{G}_i \mathbf{A}_{ij}) \mid \mathbf{G}_i \in \mathcal{G}, \mathbf{A}_{ij} \in \mathcal{M}_n(R)\} = \{\sum_{i,j} \mathbf{e}_1^T \mathbf{A}_{ij}^T \mathbf{G}_i \mathbf{A}_{ij} \mathbf{e}_1 \mid \mathbf{G}_i \in \mathcal{G}, \mathbf{A}_{ij} \in \mathcal{M}_n(R)\} = \{\sum_{i,j} \mathbf{v}_{ij}^T \mathbf{G}_i \mathbf{v}_{ij} \mid \mathbf{G}_i \in \mathcal{G}, \mathbf{v}_{ij} \in R^n\} = M_{\mathcal{G}'}$ where $\mathcal{G}' = \{\mathbf{v}^T \mathbf{G} \mathbf{v} \mid \mathbf{G} \in \mathcal{G}, \mathbf{v} \in R^n\}$. The last part now follows from (1). $\square$

In particular, if we identify the ring $\mathcal{Z}_n(R) = R \cdot \mathbf{I}_n$ with the ring R, then the set $\mathcal{M} \cap \mathcal{Z}_n(R)$, which is a quadratic module in $\mathcal{Z}_n(R)$, is identified with the set $p(\mathcal{M})$, which is a quadratic module in R.

Example 1. Let $R = \mathbb{R}[x,y]$, $n = 2$ and $\mathcal{G} = \{\begin{bmatrix} x & 1 \\ 1 & y \end{bmatrix}\}$. We claim that the quadratic module $p(\mathcal{M}^2_{\mathcal{G}})$ in R is not finitely generated.

Proof. By Lemma 1, $p(\mathcal{M}^2_{\mathcal{G}}) = M_{\mathcal{G}'}$ where $\mathcal{G}' = \{a^2 x + b^2 y + 2ab \mid a, b \in R\}$ is infinite. Suppose that $M_{\mathcal{G}'} = M_G$ for some finite set $G \subseteq R$. We may assume that $G = \{g_0, g_1, \ldots, g_k\}$ with $g_0 = 1$. Let $\succ_1$ and $\succ_2$ be the graded monomial orderings induced by $x \succ_1 y$ and $y \succ_2 x$ respectively. Since the elements of G are nonnegative on $K_G = K_{\mathcal{G}'} = \{(x,y) \in \mathbb{R}^2 \mid xy \geq 1\}$, their leading coefficients with respect to $\succ_1$ or $\succ_2$ are all nonnegative. It follows that $\deg(\sum_i t_i g_i) = \max_i \deg(t_i g_i)$ for any $t_i \in \sum R^2$. Pick any $\alpha, \beta \in \mathbb{R}$. Since $\alpha^2 x + \beta^2 y - 2\alpha\beta \in \mathcal{G}' \subseteq M_G$, there exist $t_i \in \sum R^2$ such that $\alpha^2 x + \beta^2 y - 2\alpha\beta = t_0 + t_1 g_1 + \ldots + t_k g_k$. The degree formula implies that $\deg(t_i g_i) \leq 1$ for all i. Since $t_i g_i \geq 0$ on $K_{\mathcal{G}'}$, it follows that for every $i = 1, \ldots, l$ there exist $\alpha_i, \beta_i \in \mathbb{R}^+$ and $\gamma_i \in \mathbb{R}$ such that $t_i g_i = \alpha_i^2 x + \beta_i^2 y + \gamma_i$ with $\gamma_i \geq -2\alpha_i\beta_i$. By comparing coefficients, we get that $\alpha^2 = \sum_{i=1}^l \alpha_i^2$, $\beta^2 = \sum_{i=1}^l \beta_i^2$ and $-2\alpha\beta = t_0 + \sum_{i=1}^l \gamma_i \geq \sum_{i=1}^l (-2\alpha_i\beta_i)$. It follows that $\sqrt{\sum_{i=1}^l \alpha_i^2}\sqrt{\sum_{i=1}^l \beta_i^2} \leq$

$\sum_{i=1}^{l} \alpha_i \beta_i$, hence $(\alpha_1, \ldots, \alpha_l)$ and $(\beta_1, \ldots, \beta_l)$ are colinear, $t_0 = 0$ and $\gamma_i = -2\alpha_i\beta_i$. Therefore, $\alpha^2 x + \beta^2 y - 2\alpha\beta$ is a constant multiple of an element from G. In particular, G is infinite, a contradiction. $\square$

A subset $\mathcal{T}$ of the set $\mathcal{S}_n(R)$ is a *preordering* if $\mathcal{T}$ is a quadratic module in $\mathcal{M}_n(R)$ and the set $p(\mathcal{T})$ is closed under multiplication. By Lemma 1 the set $p(\mathcal{T})$ is closed for multiplication iff the set $\mathcal{T} \cap \mathcal{Z}_n(R)$ is closed under multiplication. The smallest preordering in $\mathcal{M}_n(R)$ containing a given set $\mathcal{G} \subseteq \mathcal{S}_n(R)$ will be denoted by $\mathcal{T}_{\mathcal{G}}^n$.

In particular, a subset T of R is a preordering if $T + T \subseteq T$, $T \cdot T \subseteq T$ and $r^2 \in T$ for every $r \in R$. The smallest preordering in R which contains a given subset G of R will be denoted by T_G.

Example 2. Let $\Sigma_n(R)$ be the set of all finite sums of elements of the form $\mathbf{A}^T\mathbf{A}$ where $\mathbf{A} \in \mathcal{M}_n(R)$. We have that $\mathcal{T}_{\emptyset}^n = \mathcal{M}_{\emptyset}^n = \Sigma_n(R)$. Moreover, for every ideal I of R, $\mathcal{T}_{I \cdot \mathbf{I}_n}^n = \mathcal{M}_{I \cdot \mathbf{I}_n}^n = \mathcal{T}_{\mathcal{S}_n(I)}^n = \mathcal{M}_{\mathcal{S}_n(I)}^n = \Sigma_n(R) + \mathcal{S}_n(I)$.

Proof. To prove the first part, note that the set $p(\Sigma_n(R))$ consists of all finite sums of squares of elements from R, hence it is closed under multiplication. To prove the second part, we have to show that $\mathcal{S}_n(I) \subseteq \mathcal{M}_{I \cdot \mathbf{I}_n}^n$ and that $\Sigma_n(R) + \mathcal{S}_n(I)$ is a preordering. Namely, the second claim implies that $\mathcal{T}_{\mathcal{S}_n(I)}^n \subseteq \Sigma_n(R) + \mathcal{S}_n(I)$ while the first claim implies that $\Sigma_n(R) + \mathcal{S}_n(I) \subseteq \mathcal{M}_{I \cdot \mathbf{I}_n}^n$. Other inclusions are clear.

Pick $a \in I$ and note that for any positive integers i and j, $a\mathbf{E}_{ii} = \mathbf{E}_{ii}^T(a\mathbf{I}_n)\mathbf{E}_{ii} \in \mathcal{M}_{I \cdot \mathbf{I}_n}^n$ and $a(\mathbf{E}_{ij} + \mathbf{E}_{ji}) = (\mathbf{E}_{ii} + \mathbf{E}_{ij})^T(a\mathbf{I}_n)(\mathbf{E}_{ii} + \mathbf{E}_{ij}) + \mathbf{E}_{ii}^T(-a\mathbf{I}_n)\mathbf{E}_{ii} + \mathbf{E}_{jj}^T(-a\mathbf{I}_n)\mathbf{E}_{jj} \in \mathcal{M}_{I \cdot \mathbf{I}_n}^n$. It follows that $\mathcal{S}_n(I) \subseteq \mathcal{M}_{I \cdot \mathbf{I}_n}^n$. Let $\pi \colon R \to R/I$ be the canonical mapping and let the mapping $\pi_n \colon \mathcal{M}_n(R) \to \mathcal{M}_n(R/I)$ be defined by $\pi_n([a_{ij}]) = [\pi(a_{ij})]$. Since π_n is a $*$-homomorphism, $(\pi_n)^{-1}(\Sigma_n(R/I)) = \Sigma_n(R) + \mathcal{M}_n(I)$. By the first part, $\Sigma_n(R/I)$ is a preordering and so $\Sigma_n(R) + \mathcal{S}_n(I)$ is also a preordering. $\square$

Lemma 2. *For every subset $\mathcal{G}$ of $\mathcal{S}_n(R)$, we have that*

$$\mathcal{T}_{\mathcal{G}}^n = \mathcal{M}_{\mathcal{G} \cup (\prod \mathcal{G}' \cdot \mathbf{I}_n)}^n$$

where $\prod \mathcal{G}'$ is the set of all finite products of elements from

$$\mathcal{G}' = \{\mathbf{v}^T\mathbf{G}\mathbf{v} \mid \mathbf{G} \in \mathcal{G}, \mathbf{v} \in R^n\}.$$

Proof. The formula $(\mathbf{v}^T\mathbf{G}\mathbf{v})\mathbf{I}_n = \sum_{i=1}^n (\mathbf{v}\mathbf{e}_i^T)^T \mathbf{G} (\mathbf{v}\mathbf{e}_i^T)$, which follows from $\mathbf{I}_n = \sum_{i=1}^n \mathbf{e}_i\mathbf{e}_i^T$, implies that $\mathcal{G}' \cdot \mathbf{I}_n$ belongs to $\mathcal{M}_{\mathcal{G}}^n$, hence $\prod \mathcal{G}' \cdot \mathbf{I}_n$ belongs to $\mathcal{T}_{\mathcal{G}}^n$. Therefore $\mathcal{M}_{\mathcal{G} \cup (\prod \mathcal{G}' \cdot \mathbf{I}_n)}^n \subseteq \mathcal{T}_{\mathcal{G}}^n$. It remains to show that the set $p(\mathcal{M}_{\mathcal{G} \cup (\prod \mathcal{G}' \cdot \mathbf{I}_n)}^n) \cdot \mathbf{I}_n$ is closed under multiplication. Since

$p(\mathcal{M}^n_{\mathcal{G}\cup(\prod \mathcal{G}'\cdot \mathbf{I}_n)}) = M_{\mathcal{G}''}$ where $\mathcal{G}'' = \{\mathbf{v}^T\mathbf{T}\mathbf{v} \mid \mathbf{T} \in \mathcal{G} \cup (\prod \mathcal{G}' \cdot \mathbf{I}_n), \mathbf{v} \in R^n\} = \{\mathbf{v}^T\mathbf{T}\mathbf{v} \mid \mathbf{T} \in \mathcal{G}, \mathbf{v} \in R^n\} \cup \{\mathbf{T}\mathbf{v}^T\mathbf{v} \mid \mathbf{T} \in \prod \mathcal{G}' \cdot \mathbf{I}_n, \mathbf{v} \in R^n\} = \mathcal{G}' \cup \prod \mathcal{G}' = \prod \mathcal{G}'$ is closed under multiplication, we have that the quadratic module $\mathcal{M}^n_{\mathcal{G}\cup(\prod \mathcal{G}'\cdot \mathbf{I}_n)}$ is a preordering and hence, by minimality, equal to $\mathcal{T}^n_{\mathcal{G}}$. □

For $\mathcal{G} = \emptyset$, the preordering $\mathcal{T}^n_{\mathcal{G}} = \Sigma_n(R)$ from Example 2 has the property $\mathcal{T}^n_{\mathcal{G}}(\mathcal{T}^n_{\mathcal{G}} \cap \mathcal{Z}_n(R)) \subseteq \mathcal{T}^n_{\mathcal{G}}$. We will show now that there exist preorderings which do not satisfy this property.

Example 3. Let $R = \mathbb{R}[x, y]$, $n = 2$, $\mathbf{G} = \begin{bmatrix} x & 1 \\ 1 & y \end{bmatrix}$ and $\mathcal{G} = \{\mathbf{G}\}$. We claim that $\mathcal{T}^n_{\mathcal{G}}(\mathcal{T}^n_{\mathcal{G}} \cap \mathcal{Z}_n(R)) \not\subseteq \mathcal{T}^n_{\mathcal{G}}$.

Proof. Clearly, $x\mathbf{I}_n \in \mathcal{T}^n_{\mathcal{G}} \cap \mathcal{Z}_n(R)$ and $\mathbf{G} \in \mathcal{T}^n_{\mathcal{G}}$. We claim that $x\mathbf{G} \notin \mathcal{T}^n_{\mathcal{G}}$. Suppose that this is false. Since $\mathcal{T}^n_{\mathcal{G}} = \mathcal{M}^n_{\mathcal{G}\cup(\prod \mathcal{G}'\cdot \mathbf{I}_n)}$, there exist elements $\mathbf{A}_i, \mathbf{B}_j, \mathbf{C}_{kl} \in \mathcal{M}_2(R)$ and $t_k \in \prod \mathcal{G}'$ such that

$$x\mathbf{G} = \sum_i \mathbf{A}_i^T\mathbf{A}_i + \sum_j \mathbf{B}_j^T\mathbf{G}\mathbf{B}_j + \sum_{k,l} t_k \mathbf{C}_{kl}^T\mathbf{C}_{kl}.$$

Every element t_k is a product of the elements of the form $\mathbf{v}^T\mathbf{G}\mathbf{v} = p^2x + q^2y + 2pq$ where $p, q \in R$. By comparing the degrees, we see that all $\mathbf{A}_i$ are constant or linear, $\mathbf{B}_i$ and $\mathbf{C}_{k,l}$ are constant and each t_i is a product of one or two factors with constant p, q.

Firstly, we compare entries at position $(2, 2)$. We get that $(\mathbf{A}_i)_{21} = (\mathbf{A}_i)_{22} = 0$ and $(\sum_{k,l} t_k\mathbf{C}_{kl}^T\mathbf{C}_{kl})_{22} = xy$. Secondly, we compare entries at position $(1, 1)$ and we get that $(\sum_{k,l} t_k\mathbf{C}_{kl}^T\mathbf{C}_{kl})_{11} = 0$, which implies that $(\mathbf{A}_i)_{11}$ and $(\mathbf{A}_i)_{12}$ are constant multiples of x. Finally, we compare entries at position $(1, 2)$ and obtain a contradiction $x = 0$. □

Proposition 3. *Let N be a quadratic module in R and let $\mathfrak{N}$ be the set of all quadratic modules on $\mathcal{M}_n(R)$ whose intersection with $\mathcal{Z}_n(R)$ is equal to $N \cdot \mathbf{I}_n$. Then the smallest element of $\mathfrak{N}$ is the set*

$$N^n := \{\sum_i n_i\mathbf{A}_i^T\mathbf{A}_i \mid n_i \in N, \mathbf{A}_i \in \mathcal{M}_n(R)\}$$

and the largest element of $\mathfrak{N}$ is the set

$$\mathrm{Ind}(N) := \{\mathbf{A} \in \mathcal{S}_n(R) \mid \mathbf{v}^T\mathbf{A}\mathbf{v} \in N \text{ for all } \mathbf{v} \in R^n\}.$$

Proof. Clearly, N^n and $\mathrm{Ind}(N)$ are quadratic modules which contain $N \cdot \mathbf{I}_n$. It is also clear that $p(\sum_i n_i\mathbf{A}_i^T\mathbf{A}_i) = \sum_i(n_i \sum_j(\mathbf{A}_i)^2_{j1})$, hence $p(N^n) \subseteq N$. By Lemma 1, it follows that $N^n \cap \mathcal{Z}_n(R) = p(N)\mathbf{I}_n$. Similarly, for every $\mathbf{A} \in \mathrm{Ind}(N)$, $p(\mathbf{A}) = \mathbf{e}_1^T\mathbf{A}\mathbf{e}_1 \in N$, hence $p(\mathrm{Ind}(N)) \subseteq N$ and so $\mathrm{Ind}(N) \cap \mathcal{Z}_n(R) = N \cdot \mathbf{I}_n$. Therefore N^n and $\mathrm{Ind}(N)$ belong

to $\mathfrak{N}$. Now pick any $\mathcal{M}$ from $\mathfrak{N}$. Since $\mathcal{M}$ contains $N \cdot \mathbf{I}_n$, it also contains the smallest quadratic module in $\mathcal{M}_n(R)$ generated by $N \cdot \mathbf{I}_n$, namely N^n. On the other hand, for every $\mathbf{M} \in \mathcal{M}$ and every $\mathbf{v} \in R^n$, $(\mathbf{v}^T\mathbf{M}\mathbf{v})\mathbf{I}_n = \sum_{i=1}^n (\mathbf{v}\mathbf{e}_i^T)^T\mathbf{M}(\mathbf{v}\mathbf{e}_i^T)$ belongs to $\mathcal{M} \cap \mathcal{Z}_n(R) = N \cdot \mathbf{I}_n$, hence $\mathbf{v}^T\mathbf{M}\mathbf{v} \in N$. It follows that $\mathcal{M} \subseteq \mathrm{Ind}(N)$. $\square$

If N is a preordering in R (i.e. a quadratic module in R which is closed under multiplication), then every element of $\mathfrak{N}$ (including N^n and $\mathrm{Ind}(N)$) is a preordering in $\mathcal{M}_n(R)$.

3. Prime quadratic modules

A quadratic module $\mathcal{M}$ in $\mathcal{M}_n(R)$ is *proper* if $-\mathbf{I}_n \notin \mathcal{M}$. A proper quadratic module $\mathcal{M}$ in $\mathcal{M}_n(R)$ is *prime* if for every $\mathbf{A} \in \mathcal{S}_n(R)$ and $r \in R$ such that $\mathbf{A}r^2 \in \mathcal{M}$ we have that either $\mathbf{A} \in \mathcal{M}$ or $r \in p(\mathcal{M} \cap -\mathcal{M})$. (Equivalently, for every $\mathbf{A} \in \mathcal{S}_n(R)$ and $\mathbf{Z} \in \mathcal{Z}_n(R)$ such that $\mathbf{A}\mathbf{Z}^2 \in \mathcal{M}$ we have that either $\mathbf{A} \in \mathcal{M}$ or $\mathbf{Z} \in \mathcal{M} \cap -\mathcal{M}$.) The set $\mathrm{supp}\,\mathcal{M} := \mathcal{M} \cap -\mathcal{M}$ is called the *support* of the quadratic module $\mathcal{M}$.

Lemma 4. *For every prime quadratic module $\mathcal{M}$ the following are true:*

1. *If $\mathbf{M}_1 + \mathbf{M}_2 \in \mathrm{supp}\,\mathcal{M}$ for some $\mathbf{M}_1, \mathbf{M}_2 \in \mathcal{M}$ then $\mathbf{M}_1, \mathbf{M}_2 \in \mathrm{supp}\,\mathcal{M}$.*
2. *If $2\mathbf{A} \in \mathcal{M}$ for some $\mathbf{A} \in \mathcal{S}_n(R)$ then $\mathbf{A} \in \mathcal{M}$.*
3. *$p(\mathrm{supp}\,\mathcal{M}) \cdot \mathcal{S}_n(R) \subseteq \mathrm{supp}\,\mathcal{M}$ and $R \cdot \mathrm{supp}\,\mathcal{M} \subseteq \mathrm{supp}\,\mathcal{M}$.*
4. *If $\mathbf{A}b \in \mathrm{supp}\,\mathcal{M}$ for some $\mathbf{A} \in \mathcal{S}_n(R)$ and $b \in R$, then either $\mathbf{A} \in \mathrm{supp}\,\mathcal{M}$ or $b \in p(\mathrm{supp}\,\mathcal{M})$.*
5. *The set $p(\mathrm{supp}\,\mathcal{M})$ is a prime ideal in R.*
6. *An element $\mathbf{A} = [a_{ij}] \in \mathcal{S}_n(R)$ belongs to $\mathrm{supp}\,\mathcal{M}$ iff all a_{ij} belong to $p(\mathrm{supp}\,\mathcal{M})$. In other words, $\mathrm{supp}\,\mathcal{M} = \mathcal{S}_n(p(\mathrm{supp}\,\mathcal{M}))$.*
7. *The set $\{\mathbf{B} \in \mathcal{M}_n(R) \mid \mathbf{B}^T\mathbf{B} \in \mathrm{supp}\,\mathcal{M}\}$ is a two-sided ideal in $\mathcal{M}_n(R)$ and its intersection with $\mathcal{S}_n(R)$ is equal to $\mathrm{supp}\,\mathcal{M}$.*
8. *Let $\mathcal{G}$ be a subset of $\mathcal{M}_n(R)$ and let $\mathrm{ideal}(\mathcal{G})$ be the two-sided ideal in $\mathcal{M}_n(R)$ generated by $\mathcal{G}$. If $\mathbf{G}^T\mathbf{G} \in \mathrm{supp}\,\mathcal{M}$ for every $\mathbf{G} \in \mathcal{G}$, then $\mathrm{ideal}(\mathcal{G}) \cap \mathcal{S}_n(R) \subseteq \mathrm{supp}\,\mathcal{M}$.*

Proof. Let $\mathcal{M}$ be a prime quadratic module.

If $\mathbf{M}_1, \mathbf{M}_2 \in \mathcal{M}$ and $\mathbf{M}_1 + \mathbf{M}_2 \in \mathrm{supp}\,\mathcal{M}$, then $-\mathbf{M}_1 = \mathbf{M}_2 + (-\mathbf{M}_1 - \mathbf{M}_2) \in \mathcal{M} + \mathcal{M} \subseteq \mathcal{M}$. This proves (1).

If $2\mathbf{A} \in \mathcal{M}$ for some $\mathbf{A} \in \mathcal{S}_n(R)$, then also $4\mathbf{A} \in \mathrm{supp}\,\mathcal{M}$ since $\mathcal{M}$ is closed under addition. Since $\mathcal{M}$ is prime, $4\mathbf{A} \in \mathrm{supp}\,\mathcal{M}$ implies that either $\mathbf{A} \in \mathrm{supp}\,\mathcal{M}$ or $2 \in p(\mathrm{supp}\,\mathcal{M})$. However, $2 \in p(\mathrm{supp}\,\mathcal{M})$ implies that $-1 = 1 + (-2) \in p(\mathcal{M}) + p(\mathcal{M}) \subseteq p(\mathcal{M})$, a contradiction with the assumption that $\mathcal{M}$ is proper.

To prove the first part of (3), take any $m \in p(\operatorname{supp}\mathcal{M})$ and $\mathbf{A} \in \mathcal{S}_n(R)$ and note that the elements $(\mathbf{I}_n+\mathbf{A})^T(m\,\mathbf{I}_n)(\mathbf{I}_n+\mathbf{A})$ and $(\mathbf{I}_n-\mathbf{A})^T(m\,\mathbf{I}_n)(\mathbf{I}_n-\mathbf{A})$ belong to $\operatorname{supp}\mathcal{M}$. Therefore, their sum $(=4m\mathbf{A})$ also belongs to $\operatorname{supp}\mathcal{M}$. By (2), $m\mathbf{A} \in \operatorname{supp}\mathcal{M}$. To prove the second part of (3), take any $\mathbf{M} \in \operatorname{supp}\mathcal{M}$ and $r \in R$. Since the elements $(1+r)^2\mathbf{M}$ and $(1-r)^2\mathbf{M}$ belong to $\operatorname{supp}\mathcal{M}$, their difference $(=4r\mathbf{M})$ also belongs to $\operatorname{supp}\mathcal{M}$. By (2), $r\mathbf{M} \in \operatorname{supp}\mathcal{M}$.

To prove (4), pick $\mathbf{A} \in \mathcal{S}_n(R)$ and $b \in R$ such that $\mathbf{A}b \in \operatorname{supp}\mathcal{M}$. By (3), it follows that $\mathbf{A}b^2 \in \operatorname{supp}\mathcal{M}$. Since $\mathcal{M}$ is prime, it follows that either $\mathbf{A} \in \operatorname{supp}\mathcal{M}$ or $b \in p(\operatorname{supp}\mathcal{M})$ as claimed.

Clearly, (5) follows from (3) and (4).

If $\mathbf{A} = [a_{ij}]$ belongs to $\operatorname{supp}\mathcal{M}$, then $a_{ii} = \mathbf{e}_i^T\mathbf{A}\mathbf{e}_i \in p(\operatorname{supp}\mathcal{M})$ for all i and $a_{ii}+a_{jj}+2a_{ij} = (\mathbf{e}_i+\mathbf{e}_j)^T\mathbf{A}(\mathbf{e}_i+\mathbf{e}_j) \in p(\operatorname{supp}\mathcal{M})$ for all i and j. Hence $a_{ij} \in p(\operatorname{supp}\mathcal{M})$ for all i and j by (2) and Lemma 1. Conversely, if $a_{ij} \in p(\operatorname{supp}\mathcal{M})$ for all i and j, then $a_{ii}\mathbf{E}_{ii}$ and $a_{ij}(\mathbf{E}_{ij}+\mathbf{E}_{ji}) \in \operatorname{supp}\mathcal{M}$ by (3). Since $\mathcal{M}$ is closed under addition, it follows that $\mathbf{A} \in \operatorname{supp}\mathcal{M}$. This proves (6).

Suppose that $\mathbf{B}^T\mathbf{B} \in \operatorname{supp}\mathcal{M}$ for some $\mathbf{B} = [b_{ij}] \in \mathcal{M}_n(R)$. By (6), it follows that $b_{1i}^2+\ldots+b_{ni}^2 \in p(\operatorname{supp}\mathcal{M})$ for every $i=1,\ldots,n$. By (1) and (4), it follows that $b_{ij} \in p(\operatorname{supp}\mathcal{M})$ for all $i,j=1,\ldots,n$. Hence, $\mathbf{B} \in \mathcal{M}_n(p(\operatorname{supp}\mathcal{M}))$. Conversely, if $\mathbf{B} \in \mathcal{M}_n(p(\operatorname{supp}\mathcal{M}))$, then $\mathbf{B}^T\mathbf{B} \in \mathcal{S}_n(p(\operatorname{supp}\mathcal{M}))$ and so $\mathbf{B}^T\mathbf{B} \in \operatorname{supp}\mathcal{M}$ by (5). It follows that $\{\mathbf{B} \in \mathcal{M}_n(R) \mid \mathbf{B}^T\mathbf{B} \in \operatorname{supp}\mathcal{M}\} = \mathcal{M}_n(p(\operatorname{supp}\mathcal{M}))$ which implies both claims of (7).

Write $\mathcal{J} = \{\mathbf{B} \in \mathcal{M}_n(R) \mid \mathbf{B}^T\mathbf{B} \in \operatorname{supp}\mathcal{M}\}$. If $\mathbf{G}^T\mathbf{G} \in \operatorname{supp}\mathcal{M}$ for every $\mathbf{G} \in \mathcal{G}$, then $\mathcal{G} \subseteq \mathcal{J}$. By (7), it follows that $\operatorname{ideal}(\mathcal{G}) \subseteq \mathcal{J}$ and so $\operatorname{ideal}(\mathcal{G}) \cap \mathcal{S}_n(R) \subseteq \mathcal{J} \cap \mathcal{S}_n(R) = \operatorname{supp}\mathcal{M}$. □

For every subset $\mathcal{G}$ of $\mathcal{S}_n(R)$ write $\mathfrak{K}_{\mathcal{G}}^n$ for the set of all prime quadratic modules in $\mathcal{M}_n(R)$ which contain $\mathcal{G}$. Proposition 5 is the main result of this section. The idea for its proof comes from [9].

Proposition 5. *For every subset $\mathcal{G} \subseteq \mathcal{S}_n(R)$ there exists a subset $\tilde{\mathcal{G}} \subseteq \mathcal{M}_{\mathcal{G}}^n \cap \mathcal{Z}_n(R)$ such that $\mathfrak{K}_{\mathcal{G}}^n = \mathfrak{K}_{\tilde{\mathcal{G}}}^n$. If $\mathcal{G}$ is finite, then $\tilde{\mathcal{G}}$ can also be chosen finite.*

Proof. In the following we assume that for every $k=2,\ldots,n$, $\mathcal{S}_{k-1}(R)$ is embedded in the upper left corner of $\mathcal{S}_k(R)$ by adding zeros elsewhere.

It suffices to show that for every $k=n,\ldots,2$ and every element $\mathbf{A}$ of $\mathcal{S}_k(R)$, there exists a finite subset $\mathcal{G}_{\mathbf{A}}$ of $\mathcal{S}_{k-1}(R)$ such that $\mathcal{G}_{\mathbf{A}} \subseteq \mathcal{M}_{\mathbf{A}}$ and $\mathfrak{K}_{\mathbf{A}}^n = \mathfrak{K}_{\mathcal{G}_{\mathbf{A}}}^n$. It follows that for every subset $\mathcal{G}' \subseteq \mathcal{S}_k(R)$ the set $\mathcal{G}'' := \bigcup_{\mathbf{A}\in\mathcal{G}'} \mathcal{G}_{\mathbf{A}}$ is contained both in $\mathcal{S}_{k-1}(R)$ and $\mathcal{M}_{\mathcal{G}'}$, it satisfies

$\mathfrak{K}^n_{\mathcal{G}''} = \bigcap_{\mathbf{A}\in\mathcal{G}'} \mathfrak{K}^n_{\mathcal{G}_\mathbf{A}} = \bigcap_{\mathbf{A}\in\mathcal{G}'} \mathfrak{K}^n_\mathbf{A} = \mathfrak{K}^n_{\mathcal{G}'}$ and it is finite if $\mathcal{G}'$ is finite. The result follows by induction.

Pick $\mathbf{A} = [a_{ij}] \in \mathcal{S}_n(R)$. For every $i, j = 1, \ldots, n$ write

$$\tilde{a}_{ij} := \begin{cases} a_{ii} & \text{if } j = i \\ a_{ii} + a_{jj} + 2a_{ij} & \text{if } j \neq i \end{cases}$$

and

$$\mathbf{T}_{ij} := \begin{cases} \mathbf{I}_n & \text{if } j = i \\ \mathbf{I}_n + \mathbf{E}_{ji} & \text{if } j \neq i \end{cases}$$

Let $\mathbf{P}_{1i}$ be the permutation matrix that belongs to the transposition $(1i)$. Note that

$$\mathbf{A}_{ij} := \mathbf{P}_{1i}^T \mathbf{T}_{ij}^T \mathbf{A} \mathbf{T}_{ij} \mathbf{P}_{1i} = \begin{bmatrix} \tilde{a}_{ij} & \mathbf{b}_{ij} \\ \mathbf{b}_{ij}^T & \mathbf{C}_{ij} \end{bmatrix}$$

for some $\mathbf{b}_{ij}$ and $\mathbf{C}_{ij}$. Now write $\mathbf{B}_{ij} := \tilde{a}_{ij}(\tilde{a}_{ij}\mathbf{C}_{ij} - \mathbf{b}_{ij}^T \mathbf{b}_{ij})$ and

$$\mathbf{X}_{\pm,ij} := \begin{bmatrix} \tilde{a}_{ij} & \pm\mathbf{b}_{ij} \\ 0 & \tilde{a}_{ij}\mathbf{I}_{n-1} \end{bmatrix}$$

and observe that

$$\mathbf{X}_{-,ij}^T \mathbf{A}_{ij} \mathbf{X}_{-,ij} = \begin{bmatrix} \tilde{a}_{ij}^3 & 0 \\ 0 & \mathbf{B}_{ij} \end{bmatrix} \tag{1}$$

and

$$\mathbf{X}_{+,ij}^T \begin{bmatrix} \tilde{a}_{ij}^3 & 0 \\ 0 & \mathbf{B}_{ij} \end{bmatrix} \mathbf{X}_{+,ij} = \tilde{a}_{ij}^4 \mathbf{A}_{ij}. \tag{2}$$

If $\mathbf{A} \in \mathcal{S}_k(R)$, then the set $\mathcal{G}_\mathbf{A} := \bigcup_{i,j=1}^n \{\tilde{a}_{ij}^3, \mathbf{B}_{ij}\}$ is clearly contained in $\mathcal{S}_{k-1}(R)$. By the equality (1), it is also contained in $\mathcal{M}^n_\mathbf{A}$.

To prove that $\mathfrak{K}^n_\mathbf{A} = \mathfrak{K}^n_{\mathcal{G}_\mathbf{A}}$, it suffices to find an element $t \in \sum R^2$ such that $\mathbf{A}t \in \mathcal{M}^n_{\mathcal{G}_\mathbf{A}}$ and $\mathfrak{K}^n_{\mathbf{A}t} \subseteq \mathfrak{K}^n_\mathbf{A}$. These two properties imply that $\mathfrak{K}^n_{\mathcal{G}_\mathbf{A}} \subseteq \mathfrak{K}^n_{\mathbf{A}t} \subseteq \mathfrak{K}^n_\mathbf{A}$ and the property $\mathcal{G}_\mathbf{A} \subseteq \mathcal{M}^n_\mathbf{A}$ implies that $\mathfrak{K}^n_\mathbf{A} \subseteq \mathfrak{K}^n_{\mathcal{G}_\mathbf{A}}$. Write

$$t := \sum_{i,j=1}^n \tilde{a}_{ij}^4.$$

and note that, by the equality (2) and the definition of $\mathbf{A}_{ij}$,

$$\mathbf{A}t = \sum_{i,j=1}^n \mathbf{P}_{1i}^T (\mathbf{T}_{ij}^{-1})^T \mathbf{X}_{+,ij}^T \begin{bmatrix} \tilde{a}_{ij}^3 & 0 \\ 0 & \mathbf{B}_{ij} \end{bmatrix} \mathbf{X}_{+,ij} \mathbf{T}_{ij}^{-1} \mathbf{P}_{1i} \in \mathcal{M}^n_{\mathcal{G}_\mathbf{A}}. \tag{3}$$

Suppose now that $\mathbf{A}t \in \mathcal{M}$ for some prime quadratic module $\mathcal{M}$. Since $t \in \sum R^2$, it follows that $\mathbf{A}t^2 \in \mathcal{M}$, hence either $\mathbf{A} \in \mathcal{M}$ or $t \in p(\operatorname{supp} \mathcal{M})$. If $t \in p(\operatorname{supp} \mathcal{M})$, then by claim (1) of Lemma 4, $\tilde{a}_{ij}^4 \in p(\operatorname{supp} \mathcal{M})$ for all i, j. By claim (5) of Lemma 4, it follows that

$\tilde{a}_{ij} \in p(\operatorname{supp} \mathcal{M})$ for all i, j. Therefore, $a_{ij} \in p(\operatorname{supp} \mathcal{M})$ by claim (2) of Lemma 4. By claim (6) of Lemma 4, it follows that $\mathbf{A} \in \operatorname{supp} \mathcal{M}$. $\square$

Proposition 6 will be used in the proof of Proposition 9.

Proposition 6. *If N is a prime quadratic module in R, then* $\operatorname{Ind}(N)$ *is a prime quadratic module in $\mathcal{M}_n(R)$. Moreover,* $\operatorname{Ind}(N)$ *is the only prime quadratic module on $\mathcal{M}_n(R)$ whose intersection with $\mathcal{Z}_n(R)$ is equal to $N \cdot \mathbf{I}_n$.*

Proof. Suppose that $\mathbf{A}t^2 \in \operatorname{Ind}(N)$ for some $\mathbf{A} \in \mathcal{S}_n(R)$ and $t \in R$. It follows that $(\mathbf{v}^T\mathbf{A}\mathbf{v})t^2 = \mathbf{v}^T(\mathbf{A}t^2)\mathbf{v} \in N$ for every $\mathbf{v} \in R^n$ and $t \in R$. If N is prime, then either $\mathbf{v}^T\mathbf{A}\mathbf{v} \in N$ or $t \in \operatorname{supp} N$. If $t \notin \operatorname{supp} N$, it follows that $\mathbf{A} \in \operatorname{Ind}(N)$. If $-\mathbf{I}_n \in \operatorname{Ind}(N)$, then $-1 = \mathbf{e}_1^T(-\mathbf{I}_n)\mathbf{e}_1 \in N$, a contradiction. Therefore, $\operatorname{Ind}(N)$ is prime.

The uniqueness part follows from Proposition 5. Namely, for every $\mathbf{A} \in \mathcal{S}_n(R)$, there exists a subset $\mathcal{G}_\mathbf{A}$ of $\mathcal{Z}_n(R) \cap \mathcal{M}_\mathbf{A}$ such that $\mathfrak{K}^n_\mathbf{A} = \mathfrak{K}^n_{\mathcal{G}_\mathbf{A}}$. For every prime quadratic module $\mathcal{M}$ in $\mathcal{M}_n(R)$, it follows $\mathbf{A} \in \mathcal{M}$ iff $\mathcal{M} \in \mathfrak{K}^n_\mathbf{A}$ iff $\mathcal{M} \in \mathfrak{K}^n_{\mathcal{G}_\mathbf{A}}$ iff $\mathcal{G}_\mathbf{A} \subseteq \mathcal{M}$. Hence $\mathcal{M} = \{\mathbf{A} \in \mathcal{S}_n(R) \mid \mathcal{G}_\mathbf{A} \subseteq \mathcal{M} \cap \mathcal{Z}_n(R)\}$, i.e. $\mathcal{M}$ is uniquely determined by $\mathcal{M} \cap \mathcal{Z}_n(R)$. $\square$

In particular $N \mapsto \operatorname{Ind}(N)$ and $\mathcal{M} \mapsto p(\mathcal{M})$ give a one-to-one correspondence between prime quadratic module on R and prime quadratic modules on $\mathcal{M}_n(R)$.

Remark 1. Proposition 6 can also be proved in a more conceptual way by observing that there is a natural 1-1 correspondence between prime quadratic modules in R with support J and quadratic modules in the field $QF(R/J)$ and a natural 1-1 correspondence between prime quadratic modules in $\mathcal{M}_n(R)$ with support $\mathcal{S}_n(J)$ and quadratic modules in $\mathcal{M}_n(QF(R/J))$. Theorem 1 from [2] gives a natural 1-1 correspondence between quadratic modules in $QF(R/J)$ and quadratic modules in $\mathcal{M}_n(QF(R/J))$.

We continue with an alternative description of $\operatorname{Ind}(N)$.

Proposition 7. *For every prime quadratic module N on R, we have that*

$$\operatorname{Ind}(N) = \{\mathbf{A} \in \mathcal{S}_n(R) \mid \exists t \in R \setminus \operatorname{supp} N \colon \mathbf{A}t^2 \in N^n\}.$$

Proof. Denote the right-hand side by $\widehat{N^n}$. Clearly, $\mathbf{I}_n \in \widehat{N^n}$. If $\mathbf{A}, \mathbf{B} \in \widehat{N^n}$ then there exist $s, t \in R \setminus \operatorname{supp} N$ such that $\mathbf{A}s^2 \in N^n$ and $\mathbf{B}t^2 \in N^n$. Hence $(\mathbf{A}+\mathbf{B})s^2t^2 = (\mathbf{A}s^2)t^2 + (\mathbf{B}t^2)s^2 \in N^n$ and $st \in R \setminus \operatorname{supp} N$. If $\mathbf{D} \in \widehat{N^n}$ and $\mathbf{C} \in \mathcal{M}_n(R)$, then $\mathbf{D}u^2 \in N^n$ for some $u \in R \setminus \operatorname{supp} N$,

hence $(\mathbf{C}^T\mathbf{D}\mathbf{C})u^2 = \mathbf{C}^T(\mathbf{D}u^2)\mathbf{C} \in N^n$. Therefore, $\widehat{N^n}$ is a quadratic module.

Clearly, $N \subseteq p(\widehat{N^n})$. To prove the opposite inclusion, take any $x \cdot \mathbf{I}_n \in \widehat{N^n} \cap \mathcal{Z}_n(R)$ and pick $s \in R \setminus \operatorname{supp} N$ such that $xs^2 \cdot \mathbf{I}_n \in N^n \cap \mathcal{Z}_n(R) = N \cdot \mathbf{I}_n$. Since N is prime, it follows that $x \in N$.

To show that $\widehat{N^n}$ is prime, pick any $\mathbf{A} \in \mathcal{S}_n(R)$ and $r \in R$ such that $\mathbf{A}r^2 \in \widehat{N^n}$. Pick $t \in R \backslash \operatorname{supp} N$ such that $\mathbf{A}r^2t^2 \in N^n$. If $r \in R \backslash \operatorname{supp} N$ then also $rt \in R \setminus \operatorname{supp} N$ and so $\mathbf{A} \in \widehat{N^n}$. If $r \in \operatorname{supp} N$ then also $r \in p(\operatorname{supp} N)$.

By the uniqueness part of Lemma 6, it follows that $\widehat{N^n} = \operatorname{Ind} N$. $\square$

4. Prime quadratic modules as a topological space

For every prime quadratic module $\mathcal{M}$ in $\mathcal{M}_n(R)$, we write

$$\mathcal{M}^+ = \{\mathbf{A} \in \mathcal{S}_n(R) \quad | \quad \mathbf{v}^T\mathbf{A}\mathbf{v} \in p(\mathcal{M}) \setminus \operatorname{supp} p(\mathcal{M}) \text{ for all } \mathbf{v} \in R^n \setminus (\operatorname{supp} p(\mathcal{M}))^n\}.$$

In particular, for every prime quadratic module N in $\mathcal{M}_1(R) = R$, we have that $N^+ = N \setminus \operatorname{supp} N$ and

$$(\operatorname{Ind} N)^+ \;=\; \{\mathbf{A} \in \mathcal{S}_n(R) \mid \mathbf{v}^T\mathbf{A}\mathbf{v} \in N^+ \text{ for all } \mathbf{v} \in R^n \setminus (\operatorname{supp} N)^n\}.$$

For every subset $\mathcal{G}$ of $\mathcal{S}_n(R)$ write $\mathfrak{U}^n_{\mathcal{G}}$ for the set of all prime quadratic modules $\mathcal{M}$ on $\mathcal{M}_n(R)$ such that $\mathcal{G} \subseteq \mathcal{M}^+$.

Lemma 8. *For every prime quadratic module $\mathcal{M}$, we have that:*

1. $p(\mathcal{M}^+) = p(\mathcal{M})^+$,
2. $\mathbf{I}_n \in \mathcal{M}^+$, $\mathcal{M}^+ + \mathcal{M}^+ \subseteq \mathcal{M}^+$ *and for every* $\mathbf{A} \in \mathcal{M}^+$ *and* $\mathbf{B} \in \mathcal{M}_n(R)$ *such that* $\det \mathbf{B} \notin \operatorname{supp} p(\mathcal{M})$ *we have that* $\mathbf{B}^T\mathbf{A}\mathbf{B} \in \mathcal{M}^+$.
3. *For every subset* $\mathcal{G} \subseteq \mathcal{S}_n(R)$ *there exists a subset* $\tilde{\mathcal{G}} \subseteq \mathcal{M}_{\mathcal{G}} \cap \mathcal{Z}_n(R)$ *such that* $\mathfrak{U}^n_{\mathcal{G}} = \mathfrak{U}^n_{\tilde{\mathcal{G}}}$. *If* $\mathcal{G}$ *is finite, then so is* $\tilde{\mathcal{G}}$.

Proof. The inclusion $p(\mathcal{M}^+) \subseteq p(\mathcal{M})^+$ follows directly from the definitions of p and $\mathcal{M}^+$. To prove the opposite inclusion, it suffices to show that $r\mathbf{I}_n \in \mathcal{M}^+$ for every $r \in p(\mathcal{M})^+$. For every $\mathbf{v} = (v_1, \ldots, v_n) \in R^n$, we have that $\mathbf{v}^T(r\mathbf{I}_n)\mathbf{v} = r\sum_i v_i^2 \in p(M)$. If $\mathbf{v}^T(r\mathbf{I}_n)\mathbf{v} \in \operatorname{supp} p(\mathcal{M})$ for some $\mathbf{v}$, then either $r \in \operatorname{supp} p(\mathcal{M})$ or $\sum_i v_i^2 \in \operatorname{supp} p(\mathcal{M})$. The first case contradicts the assumption $r \in p(\mathcal{M})^+$ while the second one implies that $\mathbf{v} \in (\operatorname{supp} p(\mathcal{M}))^n$.

The first claim of (2) follows from the definition of $\mathcal{M}^+$. The second claim follows from claim (1) of Lemma 4 and the definition of $\mathcal{M}^+$. To prove the third claim pick $\mathbf{A} \in \mathcal{M}^+$ and $\mathbf{B} \in \mathcal{M}_n(R)$. If $\mathbf{B}^T\mathbf{A}\mathbf{B} \notin$

$\mathcal{M}^+$, then there exists $\mathbf{v} \in R^n$ such that $\mathbf{v}^T\mathbf{B}^T\mathbf{A}\mathbf{B}\mathbf{v} \notin p(\mathcal{M})^+$. Since $\mathbf{A} \in \mathcal{M}^+$, it follows that $\mathbf{B}\mathbf{v} \in (\operatorname{supp} p(\mathcal{M}))^n$. Since $\operatorname{supp} p(\mathcal{M})$ is an ideal, it follows that $(\det \mathbf{B})\mathbf{v} = (\operatorname{Cof} \mathbf{B})^T\mathbf{B}\mathbf{v} \in (\operatorname{supp} p(\mathcal{M}))^n$. Since $\operatorname{supp} p(\mathcal{M})$ is prime, it follows that either $\det \mathbf{B} \in \operatorname{supp} p(\mathcal{M})$ or $\mathbf{v} \in (\operatorname{supp} \mathcal{M})^n$.

The proof of assertion (3) is similar to the proof of Proposition 5. Namely, take

$$\mathbf{A} = \begin{bmatrix} a_{11} & \mathbf{b} \\ \mathbf{b}^T & \mathbf{C} \end{bmatrix}, \quad \mathbf{X}_\pm := \begin{bmatrix} a_{11} & \pm\mathbf{b} \\ 0 & a_{11}\mathbf{I}_{n-1} \end{bmatrix}, \quad \mathbf{D} = \begin{bmatrix} a_{11}^3 & 0 \\ 0 & \mathbf{B} \end{bmatrix}$$

where $\mathbf{B} = a_{11}(a_{11}\mathbf{C} - \mathbf{b}^T\mathbf{b})$ and observe that $\mathbf{X}_-^T\mathbf{A}\mathbf{X}_- = \mathbf{D}$ and $\mathbf{X}_+^T\mathbf{D}\mathbf{X}_+ = a_{11}^4\mathbf{A}$. If $\mathbf{A} \in \mathcal{M}^+$, then $a_{11} \in p(\mathcal{M})^+$ by the assertion (1). Since $\det \mathbf{X}_\pm = (a_{11})^n \in p(\mathcal{M})^+$, we can apply assertion (2) to get $\mathbf{D} \in \mathcal{M}^+$. Conversely, if $\mathbf{D} \in \mathcal{M}^+$, then $a_{11}^4\mathbf{A} \in \mathcal{M}^+$ which implies that $\mathbf{A} \in \mathcal{M}^+$. Therefore $\mathfrak{U}^n_{\mathbf{A}} = \mathfrak{U}^n_{\mathbf{D}}$. By induction, there exists a diagonal matrix $\mathbf{E} \in \mathcal{M}_n(R)$ such that $\mathfrak{U}^n_{\mathbf{A}} = \mathfrak{U}^n_{\mathbf{E}}$. Then $\tilde{\mathcal{G}}$ is the set of all diagonal entries of $\mathbf{E}$. □

Write $\mathfrak{P}(\mathcal{M}_n(R))$ for the set of all prime quadratic modules on $\mathcal{M}_n(R)$. The *Harrison topology* on $\mathfrak{P}(\mathcal{M}_n(R))$ is the topology generated by the sets $\mathfrak{U}^n_{\mathcal{G}}$ where $\mathcal{G}$ is a finite subspace of $\mathcal{S}_n(R)$. The *constructible topology* on $\mathfrak{P}(\mathcal{M}_n(R))$ is the topology generated by the sets $\mathfrak{U}^n_{\mathcal{G}}$ and $\mathfrak{K}^n_{\mathcal{G}}$ where $\mathcal{G}$ is a finite subspace of $\mathcal{S}_n(R)$.

By Proposition 5 and assertion (3) of Lemma 8, for every finite subset $\mathcal{G}$ of $\mathcal{S}_n(R)$ there exist elements $g_1, \ldots, g_k, h_1, \ldots, h_l \in R$ such that $\mathfrak{U}^n_{\mathcal{G}} = \mathfrak{U}^n_{\{g_1\cdot\mathbf{I}_n,\ldots,g_k\cdot\mathbf{I}_n\}} = \mathfrak{U}^n_{g_1\cdot\mathbf{I}_n} \cap \ldots \cap \mathfrak{U}^n_{g_k\cdot\mathbf{I}_n}$ and $\mathfrak{K}^n_{\mathcal{G}} = \mathfrak{K}^n_{\{h_1\cdot\mathbf{I}_n,\ldots,h_l\cdot\mathbf{I}_n\}} = \mathfrak{K}^n_{h_1\cdot\mathbf{I}_n} \cap \ldots \cap \mathfrak{K}^n_{h_l\cdot\mathbf{I}_n}$. Therefore, the Harrison topology is already generated by the sets $\mathfrak{U}^n_{r\cdot\mathbf{I}_n}$, $r \in R$, and the constructible topology is already generated by the sets $\mathfrak{U}^n_{r\cdot\mathbf{I}_n}$ and $\mathfrak{K}^n_{r\cdot\mathbf{I}_n}$, $r \in R$.

Proposition 9. *The mappings* $\operatorname{Ind}\colon \mathfrak{P}(R) \to \mathfrak{P}(\mathcal{M}_n(R))$, $P \mapsto \operatorname{Ind} P$, *and* $p\colon \mathfrak{P}(\mathcal{M}_n(R)) \to \mathfrak{P}(R)$, $\mathcal{Q} \mapsto p(\mathcal{Q})$, *are homeomorphisms w.r.t. the Harrison topology and also w.r.t. the constructible topology.*

Proof. Since p is the inverse of Ind, it suffices to prove the claim about Ind. Clearly, for every prime quadratic module N on R and every element $r \in R$ we have that $r \in N^+$ iff $r\mathbf{I}_n \in (\operatorname{Ind} N)^+$ and also that $r \in N$ iff $r\mathbf{I}_n \in \operatorname{Ind} N$. It follows that for every $r_1, \ldots, r_k \in R$ we have that $N \in \mathfrak{U}^1_{\{r_1,\ldots,r_k\}}$ iff $\operatorname{Ind} N \in \mathfrak{U}^n_{\{r_1\mathbf{I}_n,\ldots,r_k\mathbf{I}_n\}}$ and similarly, $N \in \mathfrak{K}^1_{\{r_1,\ldots,r_k\}}$ iff $\operatorname{Ind} N \in \mathfrak{K}^n_{\{r_1\mathbf{I}_n,\ldots,r_k\mathbf{I}_n\}}$. Hence Ind is open and continuous in both topologies. □

5. Orderings

Recall that a subset P of a unital commutative ring R is an *ordering* if $P+P \subseteq P$, $P \cdot P \subseteq P$, $P \cup -P = R$ and $P \cap -P$ is a prime ideal. Note that every ordering is a prime quadratic module and a preordering. For every homomorphism from R into a real closed field κ, the set $\phi^{-1}(\kappa^2)$, where $\kappa^2 = \sum \kappa^2$ is the only ordering in κ, is an ordering in R. Moreover, every ordering on R is of this form. Namely, for every ordering P in R write κ_P for the real closure of $QF(R/\operatorname{supp} P)$ with respect to the ordering induced by P. Note that $P = \phi_P^{-1}(\kappa_P^2)$ where $\phi_P \colon R \to \kappa_P$ is the natural homomorphism.

A subset $\mathcal{Q}$ of $\mathcal{S}_n(R)$ will be called an *ordering* if $\mathcal{Q}$ is a prime quadratic module on $\mathcal{M}_n(R)$ and the set $p(\mathcal{Q})$ is an ordering on R. The set of all orderings on $\mathcal{M}_n(R)$ will be denoted by $\operatorname{Sper}\mathcal{M}_n(R)$ and called the *real spectrum* of $\operatorname{Sper}\mathcal{M}_n(R)$. The Harrison and the constructible topology on $\operatorname{Sper}\mathcal{M}_n(R)$ are inherited from $\mathfrak{P}(\mathcal{M}_n(R))$. Proposition 9 implies that $\operatorname{Sper}\mathcal{M}_n(R)$ is homeomorphic to $\operatorname{Sper} R$ in both topologies. Since $\mathfrak{K}^n_{r\cdot\mathbf{I}_n} \cap \operatorname{Sper}\mathcal{M}_n(R) = (\operatorname{Sper}\mathcal{M}_n(R)) \setminus \mathfrak{U}^n_{-r\cdot\mathbf{I}_n}$ for every $r \in R$, it follows that for every finite subset $\mathcal{G}$ of $\mathcal{S}_n(R)$ the set $\mathfrak{K}^n_{\mathcal{G}} \cap \operatorname{Sper}\mathcal{M}_n(R)$ is closed in the relative Harrison topology.

Lemma 10. *For every real closed field κ and every homomorphism $\phi \colon R \to \kappa$, we have that*

$$\operatorname{Ind}\phi^{-1}(\kappa^2) = \phi_n^{-1}(\mathcal{S}_n(\kappa)^2) \cap \mathcal{S}_n(R)$$

where $\phi_n \colon \mathcal{M}_n(R) \to \mathcal{M}_n(\kappa)$ is defined by $\phi_n([a_{ij}]) = [\phi(a_{ij})]$ and where $\mathcal{S}_n(\kappa)^2$ is the set of all positive semidefinite matrices in $\mathcal{S}_n(\kappa)$.

Proof. Let us write $\mathcal{Q} = \phi_n^{-1}(\mathcal{S}_n(\kappa)^2) \cap \mathcal{S}_n(R)$ and $P = \phi^{-1}(\kappa^2)$. By Proposition 6, it suffices to show that the set $\mathcal{Q}$ is a prime quadratic module on $\mathcal{M}_n(R)$ such that $p(\mathcal{Q}) = P$. Clearly, $\mathbf{I}_n \in \mathcal{Q}$ and $\mathcal{Q}+\mathcal{Q} \subseteq \mathcal{Q}$. If $\mathbf{A} \in \mathcal{Q}$ and $\mathbf{B} \in \mathcal{M}_n(R)$, then $\phi_n(\mathbf{B}^T\mathbf{A}\mathbf{B}) = \phi_n(\mathbf{B})^T\phi_n(\mathbf{A})\phi_n(\mathbf{B}) \in \phi_n(\mathbf{B})^T\mathcal{S}_n(\kappa)^2\phi_n(\mathbf{B}) \subseteq \mathcal{S}_n(\kappa)^2$, hence $\mathbf{B}^T\mathbf{A}\mathbf{B} \in \mathcal{Q}$.

To show that $\mathcal{Q}$ is prime, pick $\mathbf{A} \in \mathcal{S}_n(R)$ and $t \in R$ such that $\mathbf{A}t^2 \in \mathcal{Q}$. It follows that $\phi_n(\mathbf{A})\phi(t)^2 \in \mathcal{S}_n(\kappa)^2$. Hence, either $\phi(t) = 0$ or $\phi_n(\mathbf{A}) \in \mathcal{S}_n(\kappa)^2$. In the first case, we have that $t\,\mathbf{I}_n \in \operatorname{supp}\mathcal{Q}$, and in the second case that $\mathbf{A} \in \mathcal{Q}$.

Pick $\mathbf{A} \in \mathcal{Q}$. It follows that $\phi(p(\mathbf{A})) = \phi(\mathbf{e}_1^T\mathbf{A}\mathbf{e}_1) = \mathbf{e}_1^T\phi_n(\mathbf{A})\mathbf{e}_1 \subseteq \mathbf{e}_1^T\mathcal{S}_n(\kappa)^2\mathbf{e}_1 \subseteq \kappa^2$, hence $p(\mathbf{A}) \in P$. Conversely, take any $b \in P$ and note that $\phi_n(b\,\mathbf{I}_n) = \phi(b)\mathbf{I}_n \in \kappa^2 \cdot \mathbf{I}_n \subseteq \mathcal{S}_n(\kappa)^2$. Hence, $b\,\mathbf{I}_n \in \mathcal{Q}$ and so $b \in p(\mathcal{Q})$. $\square$

In summary, every ordering $\mathcal{Q}$ on $\mathcal{M}_n(R)$ is of the form

$$\mathcal{Q} = \operatorname{Ind}(P) = \widehat{P^n} = ((\phi_P)_n)^{-1}(\mathcal{S}_n(\kappa_P)^2) \cap \mathcal{S}_n(R)$$

where $P = p(\mathcal{Q})$ is an ordering on R. It follows that

$$\mathcal{Q}^+ = ((\phi_P)_n)^{-1}((\mathcal{S}_n(\kappa_P)^2)^+) \cap \mathcal{S}_n(R)$$

where $(\mathcal{S}_n(\kappa_P)^2)^+$ is the set of all positive definite matrices over κ_P.

Corollary 11. *For every $\mathbf{A} \in \mathcal{S}_n(R)$ and every ordering P on R, the following are equivalent:*

1. $\mathbf{A} \in \operatorname{Ind}(P)$,
2. *all principal minors of* $\mathbf{A}$ *belong to* P,
3. *all coefficients of the polynomial* $\det(\mathbf{A} + \lambda \mathbf{I}_n)$ *belong to* P.

Moreover, the following are equivalent:

1. $\mathbf{A} \in \operatorname{Ind}(P)^+$,
2. $\mathbf{A} \in \operatorname{Ind}(P)$ *and* $\det \mathbf{A} \in P^+$,
3. *all leading principal minors of* $\mathbf{A}$ *belong to* P^+.

Corollary 11 follows from Lemma 10 and the usual characterizations of positive semidefinite and positive definite matrices over real closed fields.

For every real closed field κ write $V_\kappa(R)$ for the set of all ring homomorphisms from R to κ.

Theorem 12. *(Artin-Lang Theorem) If R is a finitely generated $\mathbb{R}$-algebra, then the mapping*

$$i \colon V_{\mathbb{R}}(R) \to \operatorname{Sper} \mathcal{M}_n(R), \quad \phi \mapsto \phi_n^{-1}(\mathcal{S}_n(\mathbb{R})^2) \cap \mathcal{S}_n(R)$$

is one-to-one and its image is dense in the constructible topology.

Proof. By Lemma 10, i is the compositum of the mapping $j \colon V_{\mathbb{R}}(R) \to \operatorname{Sper} R$, $j(\phi) = \phi^{-1}(\mathbb{R}^2)$, and the mapping $\operatorname{Ind} \colon \operatorname{Sper} R \to \operatorname{Sper} \mathcal{M}_n(R)$. Since Ind is homeomorphism with respect to the constructible topologies on $\operatorname{Sper} R$ and $\operatorname{Sper} \mathcal{M}_n(R)$, the theorem follows from the usual Artin-Lang theorem [5, 2.4.3. Theorem]. □

6. Stellensätze

In this section, we will prove a generalization of the Krivine-Stengle theorem whose special case is the result that was announced in the Introduction.

Recall that an *affine* $\mathbb{R}$*-algebra* is a finitely generated commutative unital $\mathbb{R}$-algebra.

Theorem 13. *(Positivdefinitheitsstellensatz) For every finite subset $\mathcal{G}$ of $\mathcal{S}_n(R)$ and every element $\mathbf{F} \in \mathcal{S}_n(R)$, the following are equivalent:*

(1) *For every real closed field* κ *and every* $\phi \in V_\kappa(R)$ *such that* $\phi_n(\mathbf{G})$ *is positive semidefinite for every* $\mathbf{G} \in \mathcal{G}$*, we have that* $\phi_n(\mathbf{F})$ *is positive definite.*

(1') *For every ordering* $\mathcal{Q} \in \operatorname{Sper} \mathcal{M}_n(R)$ *which contains* $\mathcal{G}$*, we have that* $\mathbf{F} \in \mathcal{Q}^+$*.*

(2) *There exist* $\mathbf{B}, \mathbf{C} \in \mathcal{T}^n_{\mathcal{G}}$ *such that* $\mathbf{F}(\mathbf{I}_n + \mathbf{B}) = (\mathbf{I}_n + \mathbf{B})\mathbf{F} = \mathbf{I}_n + \mathbf{C}$*.*

(2') *There exist* $\mathbf{B}, \mathbf{C} \in \mathcal{T}^n_{\mathcal{G}}$ *such that* $\mathbf{F}\mathbf{B} = \mathbf{B}\mathbf{F} = \mathbf{I}_n + \mathbf{C}$*.*

(3) *There exist* $t \in p(\mathcal{T}^n_{\mathcal{G}})$ *and* $\mathbf{V} \in \mathcal{T}^n_{\mathcal{G}}$ *such that* $\mathbf{F}(1+t) = \mathbf{I}_n + \mathbf{V}$*.*

(3') *There exist* $t \in p(\mathcal{T}^n_{\mathcal{G}})$ *and* $\mathbf{V} \in \mathcal{T}^n_{\mathcal{G}}$ *such that* $\mathbf{F}t = \mathbf{I}_n + \mathbf{V}$*.*

If R *is an affine* $\mathbb{R}$*-algebra, then assertions (1)-(3') are equivalent to*

(1") *For every* $\phi \in V_{\mathbb{R}}(R)$ *such that* $\phi_n(\mathbf{G})$ *is positive semidefinite for every* $\mathbf{G} \in \mathcal{G}$*, we have that* $\phi_n(\mathbf{F})$ *is positive definite.*

Proof. The equivalence of (1) and (1') follows from the comments after Lemma 10 and the equivalence of (1') and (1") follows from Theorem 12. Clearly, (3) implies (2) and (3') and either (2) or (3') implies (2').

To prove that (2') implies (1), note that for every $\phi \in V_\kappa(R)$ such that $\phi_n(\mathbf{G})$ is positive semidefinite for every $\mathbf{G} \in \mathcal{G}$, we have that $\phi_n(\mathbf{B})$ and $\phi_n(\mathbf{C})$ are positive semidefinite. Moreover, the relation $\phi_n(\mathbf{F})\phi_n(\mathbf{B}) = \phi_n(\mathbf{B})\phi_n(\mathbf{F}) = \mathbf{I}_n + \phi_n(\mathbf{C})$ implies that $\phi_n(\mathbf{B})$ is positive definite. It follows that $\phi_n(\mathbf{F}) = \phi_n(\mathbf{B})^{-1}(\mathbf{I}_n + \phi_n(\mathbf{C})) = \phi_n(\mathbf{B})^{-1/2}\phi_n(\mathbf{I}_n + \phi_n(\mathbf{C}))\phi_n(\mathbf{B})^{-1/2}$ is positive definite.

The proof that (1) implies (3) is an obvious generalization of the proof of the main theorem from [1]. We summarize it here for the sake of completeness.

Suppose that (1) is true. By Proposition 5, we can pick a finite set $\tilde{\mathcal{G}} \subseteq \mathcal{M}^n_{\mathcal{G}} \cap \mathcal{Z}_n(R)$ such that $\mathfrak{K}^n_{\mathcal{G}} = \mathfrak{K}^n_{\tilde{\mathcal{G}}}$. Note that $\mathcal{T}^n_{\tilde{\mathcal{G}}} \subseteq \mathcal{T}^n_{\mathcal{G}}$. Pick any real closed field κ and any $\phi \in V_\kappa(R)$ such that $\phi(g) \geq 0$ for every $g \in \tilde{\mathcal{G}}$. Since $\mathfrak{K}^n_{\mathcal{G}} = \mathfrak{K}^n_{\tilde{\mathcal{G}}}$, it follows that $\phi_n(\mathbf{G})$ is positive semidefinite for every $\mathbf{G} \in \mathcal{G}$. By (1), it follows that $\phi_n(\mathbf{F})$ is positive definite. If we write

$$\mathbf{F} = \begin{bmatrix} f_{11} & \mathbf{g} \\ \mathbf{g}^T & \mathbf{H} \end{bmatrix}$$

then clearly $\phi(f_{11}) > 0$ and $\phi_{n-1}(f_{11}\mathbf{H} - \mathbf{g}^T\mathbf{g})$ is positive definite.

By [5, 2.5.2 Abstract Positivstellensatz], there exist $t, t' \in T_{\tilde{\mathcal{G}}}$ such that $f_{11}t = 1 + t'$. Note that $s_1 := t + t'$ and $u_1 := t' + f_{11}^2 t$ belong to $T_{\tilde{\mathcal{G}}}$ and satisfy

$$(1 + s_1)f_{11} = 1 + u_1.$$

By induction, there exist $s \in T_{\tilde{\mathcal{G}}}$ and $\mathbf{U} \in \mathcal{T}^{n-1}_{\tilde{\mathcal{G}}}$ such that

$$(1 + s)(f_{11}\mathbf{H} - \mathbf{g}^T\mathbf{g}) = \mathbf{I}_{n-1} + \mathbf{U}.$$

Write

$$\begin{array}{rcl}
\tilde{\mathbf{g}} & = & (1+s_1)\mathbf{g}, \\
c & = & \tilde{\mathbf{g}}\tilde{\mathbf{g}}^T \in T_{\tilde{\mathcal{G}}}, \\
\mathbf{S} & = & c\,\mathbf{I}_{n-1} - \tilde{\mathbf{g}}^T\tilde{\mathbf{g}} \in \mathcal{T}_{\tilde{\mathcal{G}}}^{n-1}, \\
v & = & 1+c, \\
d & = & v(1+u_1)^2 - 1 \in T_{\tilde{\mathcal{G}}}, \\
\mathbf{D} & = & (v(1+u_1)^2 + v^2(2u_1+u_1^2))\mathbf{I}_{n-1} + (v+1)\mathbf{S} \in \mathcal{T}_{\tilde{\mathcal{G}}}^{n-1}, \\
e & = & (1+s)(1+u_1)^2 - 1 \in T_{\tilde{\mathcal{G}}}, \\
\mathbf{E} & = & (1+s_1)^2(\mathbf{I}_{n-1}+\mathbf{U}) - \mathbf{I}_{n-1} \in \mathcal{T}_{\tilde{\mathcal{G}}}^{n-1}, \\
\mathbf{R} & = & \begin{bmatrix} 1+u_1 & \tilde{\mathbf{g}} \\ 0 & (1+u_1)\mathbf{I}_{n-1} \end{bmatrix}, \\
\mathbf{Z} & = & \begin{bmatrix} v(1+u_1) & (1+v)\tilde{\mathbf{g}} \\ 0 & 0 \end{bmatrix}
\end{array}$$

and note that

$$v(1+v)(1+s)(1+s_1)(1+u_1)^3 \begin{bmatrix} f_{11} & \mathbf{g} \\ \mathbf{g}^T & \mathbf{H} \end{bmatrix} =$$

$$= \mathbf{I}_n + \begin{bmatrix} d & 0 \\ 0 & \mathbf{D} \end{bmatrix} + v(1+v)\mathbf{R}^T \begin{bmatrix} e & 0 \\ 0 & \mathbf{E} \end{bmatrix} \mathbf{R} + \mathbf{Z}^T\mathbf{Z} \in \mathbf{I}_n + \mathcal{T}_{\tilde{\mathcal{G}}}^n.$$

Clearly, $v(1+v)(1+s)(1+s_1)(1+u_1)^3 \in 1 + T_{\tilde{\mathcal{G}}} \subseteq p(\mathbf{I}_n + \mathcal{T}_{\mathcal{G}}^n)$ and $\mathbf{I}_n + \mathcal{T}_{\tilde{\mathcal{G}}}^n \subseteq \mathbf{I}_n + \mathcal{T}_{\mathcal{G}}^n$. □

We continue with a generalization of Krivine-Stengle Nichtnegativstellensatz.

Theorem 14. *(Positivsemidefinitheitsstellensatz) For every finite subset $\mathcal{G}$ of $\mathcal{S}_n(R)$ and every $\mathbf{F} \in \mathcal{S}_n(R)$ the following are equivalent:*

(1) *For every real closed field κ and every $\phi \in V_\kappa(R)$ such that $\phi_n(\mathbf{G})$ is positive semidefinite for every $\mathbf{G} \in \mathcal{G}$, we have that $\phi_n(\mathbf{F})$ is positive semidefinite.*

(1') *Every ordering on $\mathcal{M}_n(R)$ which contains $\mathcal{G}$ also contains $\mathbf{F}$.*

(2) *There exist $k \in \mathbb{N}$ and $\mathbf{B}, \mathbf{C} \in \mathcal{T}_{\mathcal{G}}^n$ such that $\mathbf{FB} = \mathbf{BF} = \mathbf{F}^{2k} + \mathbf{C}$.*

If R is an affine $\mathbb{R}$-algebra, then (1), (1') and (2) are equivalent to

(1") *For every $\phi \in V_{\mathbb{R}}(R)$ such that $\phi_n(\mathbf{G})$ is positive semidefinite for every $\mathbf{G} \in \mathcal{G}$, $\phi_n(\mathbf{F})$ is also positive semidefinite.*

Proof. The equivalence of (1) and (1') follows from the comments after Lemma 10. The equivalence of (1') and (1") follows from Theorem 12.

To prove that (2) implies (1) note that the relation $\mathbf{FB} = \mathbf{BF} = \mathbf{F}^{2k} + \mathbf{C}$ implies that $\mathbf{C}$ also commutes with $\mathbf{F}$ and $\mathbf{B}$. Pick a homomorphism ϕ from R into a real closed field κ such that $\phi_n(\mathbf{G})$ is positive semidefinite for every $\mathbf{G} \in \mathcal{G}$. Note that $\phi_n(\mathbf{B})$ and $\phi_n(\mathbf{C})$ are also positive semidefinite because they belong to $\mathcal{T}_{\mathcal{G}}^n$. Clearly $V_1 := \operatorname{Im} \phi_n(\mathbf{F})$ and $V_2 := \operatorname{Ker} \phi_n(\mathbf{F})$ are subspaces of κ^n which satisfy $V_1 \oplus V_2 = \kappa^n$. It is also clear that V_1 and V_2 are invariant for $\phi_n(\mathbf{F})$, $\phi_n(\mathbf{B})$ and $\phi_n(\mathbf{C})$. Write $\mathbf{F}_i = \phi_n(\mathbf{F})|_{V_i}$ and similarly for $\mathbf{B}$ and $\mathbf{C}$. Clearly, $\mathbf{F}_1$ is invertible and $\mathbf{F}_2 = 0$. Since $\phi_n(\mathbf{B})$ and $\phi_n(\mathbf{C})$ are positive semidefinite so are $\mathbf{B}_1$ and $\mathbf{C}_1$. It follows that $\mathbf{F}_1^{2k} + \mathbf{C}_1$ is positive semidefinite and invertible, so that $\mathbf{F}_1\mathbf{B}_1$ is also positive semidefinite and invertible. It follows that $\mathbf{B}_1$ is invertible. Since $\mathbf{F}_1 = (\mathbf{F}_1^{2k} + \mathbf{C}_1)\mathbf{B}_1^{-1}$ is a product of two commuting positive semidefinite matrices, it is positive semidefinite. Therefore $\phi_n(\mathbf{F}) = \mathbf{F}_1 \oplus 0$ is positive semidefinite as claimed.

It remains to show that (1) implies (2). By Proposition 5, we can pick a finite set $\tilde{\mathcal{G}} \subseteq \mathcal{M}_{\mathcal{G}}^n \cap \mathcal{Z}_n(R)$ such that $\mathfrak{K}_{\mathcal{G}}^n = \mathfrak{K}_{\tilde{\mathcal{G}}}^n$. We identify $\tilde{\mathcal{G}}$ with $p(\tilde{\mathcal{G}}) \subseteq R \subseteq R'$ where $R' = R[\lambda]/(\det(\mathbf{F} - \lambda \mathbf{I}_n))$. For every homomorphism $\phi \colon R' \to \kappa$ where κ is a real closed field the following is true: if $\phi(g) \geq 0$ for every $g \in \tilde{\mathcal{G}}$, then $\phi(\bar{\lambda}) \geq 0$. By [5, 2.5.2 Abstract Positivstellensatz], there exist $l \in \mathbb{N}$ and $p(\bar{\lambda}), q(\bar{\lambda}) \in T_{\tilde{\mathcal{G}}}^{R'}$ such that $\bar{\lambda} p(\bar{\lambda}) = \bar{\lambda}^{2l} + q(\bar{\lambda})$. By the Cayley-Hamilton Theorem, the natural homomorphism from $R[\lambda]$ to $R[F] \subset \mathcal{M}_n(R)$ factors through R'. It follows that $\mathbf{F}p(\mathbf{F}) = \mathbf{F}^{2l} + q(\mathbf{F})$ and $p(\mathbf{F}), q(\mathbf{F}) \in \mathcal{T}_{\tilde{\mathcal{G}}}^{R[\mathbf{F}]} \subseteq \mathcal{T}_{\tilde{\mathcal{G}}}^n \subseteq \mathcal{T}_{\mathcal{G}}^n$. Take $\mathbf{B} = p(\mathbf{F})$ and $\mathbf{C} = q(\mathbf{F})$. $\square$

Remark 2. We can also give a less abstract but slightly longer proof of the direction (1) $\Rightarrow$ (2) which is based on the observation that every ordering on $R[\lambda]$ which contains $\tilde{\mathcal{G}} \cup \{-\lambda\}$, also contains the element $\det(\mathbf{F} - \lambda \mathbf{I}_n) - (-\lambda)^n \in R[\lambda]$.

Remark 3. Theorem 14 does not seem to imply the Artin's theorem for matrix polynomials because the element $\mathbf{B}$ in its assertion (2) may not be central. Recall that Artin's theorem for matrix polynomials says that for every $\mathbf{A} \in \mathcal{S}_n(\mathbb{R}[x_1, \ldots, x_d])$ which is positive semidefinite in every $x \in \mathbb{R}^d$ there exists a nonzero $c \in \mathbb{R}[x_1, \ldots, x_d]$ such that $\mathbf{A}c^2 \in \Sigma_n(\mathbb{R}[x_1, \ldots, x_d])$. It was proved independently in [3] and [6]. For the first constructive proof see [9]. We can deduce it from the formula (3) in the proof of Proposition 5.

The following example shows that there exist $\mathbf{F}$ and $\mathcal{G}$ such that no element $\mathbf{B}$ from the assertion (2) of Theorem 14 is central.

Example 4. Take $\mathcal{G} = \{x^3\}$ and

$$\mathbf{F} = \begin{bmatrix} x & 0 \\ 0 & 1 \end{bmatrix}.$$

Clearly, $\mathbf{F}$ is positive semidefinite on $\mathfrak{K}_{\mathcal{G}}$. However there is no (central!) $b \in T_S$ such that $\mathbf{F}b = \mathbf{F}^{2k} + \mathbf{C}$ for some $k \in \mathbb{N}$ and $\mathbf{C} = [c_{ij}] \in \mathcal{T}_{\mathcal{G}}^n$. Namely, if such a b exists, then $xb = x^{2k} + c_{11}$ and $b = 1 + c_{22}$ for some $c_{11} = u_1 + x^3 v_1$ and $c_{22} = u_2 + x^3 v_2$ with $u_i, v_i \in \sum \mathbb{R}[x]^2$, then $x(1 + u_2(x) + x^3 v_2(x)) = x^{2k} + u_2(x) + x^3 v_2(x)$. Since x divides $x^{2k} + u_2(x)$ which belongs to $\sum \mathbb{R}[x]^2$, it follows that also x^2 divides $x^{2k} + u_2(x)$. After canceling x on both sides, we get that the right-hand side is divisible by x while the left-hand side is not.

If we take $\mathbf{F} = -\mathbf{I}_n$ in Theorem 14, we obtain the following result (which can also be proved more directly):

Corollary 15. *For every finite subset $\mathcal{G}$ of $\mathcal{S}_n(R)$, the following are equivalent:*

- (1) *There is no homomorphism ϕ from R into a real closed field such that $\phi_n(\mathbf{G})$ is positive semidefinite for every $\mathbf{G} \in \mathcal{G}$.*
- (1') *There is no ordering on $\mathcal{M}_n(R)$ which contains $\mathcal{G}$.*
- (2) $-\mathbf{I}_n \in \mathcal{T}_{\mathcal{G}}^n$.

If R is an affine $\mathbb{R}$-algebra, then (1), (1') and (2) are equivalent to

- (1") *There is no $\phi \in V_{\mathbb{R}}(R)$ such that $\phi_n(\mathbf{G})$ is positive semidefinite for every $\mathbf{G} \in \mathcal{G}$.*

If we replace the set $\mathcal{G}$ in Corollary 15 with the set $\mathcal{G} \cup \{-\mathbf{F}\}$, we get the following:

Corollary 16. *(Nichtnegativsemidefinitheitsstellensatz) For every finite subset $\mathcal{G}$ of $\mathcal{S}_n(R)$ and every $\mathbf{F} \in \mathcal{S}_n(R)$ the following are equivalent:*

- (1) *For every real closed field κ and every $\phi \in V_\kappa(R)$ such that $\phi_n(\mathbf{G})$ is positive semidefinite for every $\mathbf{G} \in \mathcal{G}$, we have that $\phi_n(\mathbf{F})$ is not negative semidefinite.*
- (1') *Every ordering on $\mathcal{M}_n(R)$ which contains $\mathcal{G}$ does not contain $-\mathbf{F}$.*
- (2) $-\mathbf{I}_n \in \mathcal{T}_{\mathcal{G} \cup \{-\mathbf{F}\}}^n$.

If R is an affine $\mathbb{R}$-algebra, then (1), (1') and (2) are equivalent to

- (1") *For every $\phi \in V_{\mathbb{R}}(R)$ such that $\phi_n(\mathbf{G})$ is positive semidefinite for every $\mathbf{G} \in \mathcal{G}$, $\phi_n(\mathbf{F})$ is not negative semidefinite.*

By a slight modification of the proof of Theorem 14 (replace the Krivine-Stengle Nichtnegativstellensatz for R' with the Nullstellensatz) we get the following generalization of Krivine-Stengle Nullstellensatz.

Theorem 17. *(Semialgebraic Nullstellensatz) For every finite subset $\mathcal{G}$ of $\mathcal{S}_n(R)$ and every $\mathbf{F} \in \mathcal{S}_n(R)$ the following are equivalent:*

(1) *For every real closed field κ and every $\phi \in V_\kappa(R)$ such that $\phi_n(\mathbf{G})$ is positive semidefinite for every $\mathbf{G} \in \mathcal{G}$, we have that $\phi_n(\mathbf{F}) = 0$.*

(1') *For every ordering $Q \in \operatorname{Sper} \mathcal{M}_n(R)$ which contains $\mathcal{G}$, we have that $\mathbf{F} \in \operatorname{supp} \mathcal{Q}$.*

(2) *There exists $k \in \mathbb{N}$ such that $-\mathbf{F}^{2k} \in \mathcal{T}_\mathcal{G}^n$.*

If R is an affine $\mathbb{R}$-algebra, then (1), (1') and (2) are equivalent to

(1") *For every $\phi \in V_\mathbb{R}(R)$ such that $\phi_n(\mathbf{G})$ is positive semidefinite for every $\mathbf{G} \in \mathcal{G}$, we have that $\phi_n(\mathbf{F}) = 0$.*

For $n = 1$, semialgebraic Nullstellensatz follows from the Nichtnegativstellensatz by replacing $\mathbf{F}$ with $-\mathbf{F}^T\mathbf{F}$. This does not work here even if the element $\mathbf{B}$ from the assertion (2) of Theorem 14 is central, see Example 3.

Corollary 18. *(Real Nullstellensatz) For every finite subset $\mathcal{G}$ of $\mathcal{M}_n(R)$ and every $\mathbf{F} \in \mathcal{M}_n(R)$ the following are equivalent:*

(1) *For every real closed field κ and for every $\phi \in V_\kappa(R)$ such that $\phi_n(\mathbf{G}) = 0$ for every $\mathbf{G} \in \mathcal{G}$, we have that $\phi_n(\mathbf{F}) = 0$.*

(1') *For every ordering $\mathcal{Q} \in \operatorname{Sper} \mathcal{M}_n(R)$ such that $\mathbf{G}^T\mathbf{G} \in \operatorname{supp} \mathcal{Q}$ for every $\mathbf{G} \in \mathcal{G}$, we have that $\mathbf{F}^T\mathbf{F} \in \operatorname{supp} \mathcal{Q}$.*

(2) *There exists $l \in \mathbb{N}$ such that $-(\mathbf{F}^T\mathbf{F})^l \in \Sigma_n(R) + \operatorname{ideal}(\mathcal{G})$ where $\operatorname{ideal}(\mathcal{G})$ is the two-sided ideal in $\mathcal{M}_n(R)$ generated by $\mathcal{G}$.*

If R is an affine $\mathbb{R}$-algebra, then (1), (1') and (2) are equivalent to

(1") *For every $\phi \in V_\mathbb{R}(R)$ such that $\phi_n(\mathbf{G}) = 0$ for every $\mathbf{G} \in \mathcal{G}$, we have that $\phi_n(\mathbf{F}) = 0$.*

Proof. Clearly, (1) is equivalent to the following:

(*) For every real closed field κ and every $\phi \in V_\kappa(R)$ such that $\phi_n(\mathbf{G}^T\mathbf{G}) = 0$ for every $\mathbf{G} \in \mathcal{G}$, we have that $\phi_n(\mathbf{F}^T\mathbf{F}) = 0$.

By the comment after Lemma 10, (*) is equivalent to (1'). By Theorem 12, (1') is equivalent to a special case of (*) for $\kappa = \mathbb{R}$. The latter is clearly equivalent to (1").

For the implication (1) $\Rightarrow$ (2), we use Theorem 17 with $\mathcal{G}' = \{-\mathbf{G}^T\mathbf{G} \mid \mathbf{G} \in \mathcal{G}\}$ instead of $\mathcal{G}$ and $\mathbf{F}^T\mathbf{F}$ instead of $\mathbf{F}$. We get that for some positive integer k, $-(\mathbf{F}^T\mathbf{F})^{2k} \in \mathcal{T}_{\mathcal{G}'}^n$. Clearly, $\mathcal{T}_{\mathcal{G}'}^n \subseteq \Sigma_n(R) + \operatorname{ideal}(\mathcal{G}') \subseteq \Sigma_n(R) + \operatorname{ideal}(\mathcal{G})$, hence $-(\mathbf{F}^T\mathbf{F})^{2k} \in \Sigma_n(R) + \operatorname{ideal}(\mathcal{G})$.

Conversely, suppose that (2) is true and pick a homomorphism ϕ from R into a real closed field κ such that $\phi_n(\mathbf{G}) = 0$ for every $\mathbf{G} \in \mathcal{G}$. It follows that $\phi_n(\Sigma_n(R) + \text{ideal}(\mathcal{G})) \subseteq \mathcal{S}_n(\kappa)^2$. In particular, $\phi_n(-(\mathbf{F}^*\mathbf{F})^{2k}) \in \mathcal{S}_n(\kappa)^2$, and so $\phi_n(\mathbf{F}^*\mathbf{F}) = 0$, proving (1). $\square$

References

[1] J. Cimprič, Strict Positivstellensätze for matrix polynomials with scalar constraints, to appear in Linear Algebra and its Application.

[2] J. Cimprič, Formally real involutions on central simple algebras, Comm. Algebra **36** (2008), 165-178.

[3] D. Gondard, P. Ribenboim, Le 17e probleme de Hilbert pour les matrices, Bull. Sci. Math. (2) **98** (1974), no. 1, 49–56.

[4] J.-L. Krivine, Anneaux préordonnés. J. Analyse Math. **12** (1964), 307–326.

[5] M. Marshall, Positive polynomials and sums of squares. Mathematical Surveys and Monographs, 146. American Mathematical Society, Providence, RI, 2008. xii+187 pp. ISBN: 978-0-8218-4402-1; 0-8218-4402-4

[6] C. Procesi, M. Schacher, A non-commutative real Nullstellensatz and Hilbert's 17th problem, Ann. Math. **104** (1976), 395-406.

[7] B. Reznick, On the absence of uniform denominators in Hilbert's 17th problem, Proc. Amer. Math. Soc. 133 (2005), no. 10, 2829-2834.

[8] Y. Savchuk, K. Schmüdgen, Positivstellensätze for Algebras of Matrices, arXiv:1004.1529 (Preprint, April 2010)

[9] K. Schmüdgen, Noncommutative real algebraic geometry—some basic concepts and first ideas. Emerging applications of algebraic geometry, 325–350, IMA Vol. Math. Appl., 149, Springer, New York, 2009.

[10] G. Stengle, A Nullstellensatz and a Positivstellensatz in Semialgebraic Geometry. Math. Ann. **207** (1974), 87–97.

Jaka Cimprič, University of Ljubljana, Faculty of Math. and Phys., Dept. of Math., Jadranska 19, SI-1000 Ljubljana, Slovenija. E-mail: cimpric@fmf.uni-lj.si. www page: http://www.fmf.uni-lj.si/~cimpric.